CITRIX®

# **Un nuevo enfoque de la eficacia de la seguridad:** Cómo reducir y gestionar el riesgo de su negocio

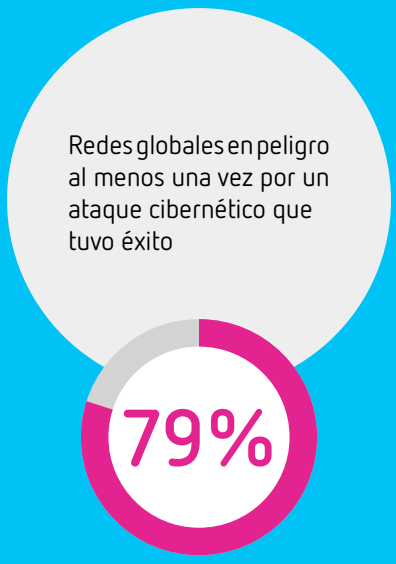
# Introducción

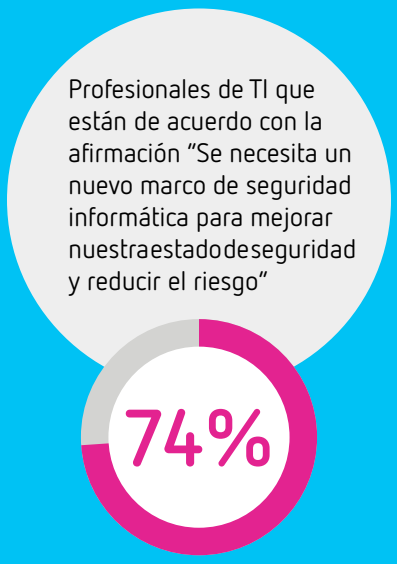
Cada día, los empleados y los clientes implementan más aplicaciones en más dispositivos, y se conectan a las redes corporativas desde un número casi infinito de lugares.

En este nuevo mundo de aplicaciones en todas partes y usuarios en cualquier lugar, TI y los responsables en seguridad encuentran niveles de riesgo cada vez mayores.

Se enfrentan a una mayor exposición a las brechas de seguridad, causadas en parte por el enorme reto de ofrecer servicios para soluciones de seguridad dispares, con varias consolas de administración y políticas incoherentes. Deben lidiar con áreas de ataque ampliadas que dan a los atacantes más lugares para encontrar datos y robar las credenciales de los usuarios. Carecen de las herramientas para correlacionar e interpretar los volúmenes cada vez mayores de datos de amenazas. Y deben superar la complejidad creciente de administrar las infraestructuras que se extienden por numerosos centros de datos y diferentes plataformas cloud en todo el mundo.

Los datos revelan la verdad: las brechas de datos están aumentando, ninguna red está a salvo de ataques de sofisticados adversarios y las organizaciones de TI carecen de confianza en su capacidad para defender a sus usuarios, aplicaciones y datos.


Fuentes:
ITRC Data Breach Report 2016, Identity Theft Resource Center
2017 Cyberthreat Defense Report, CyberEdge Group, LLC
The Need for a New IT Security Architecture, Ponemon Institute LLC

# Un nuevo enfoque de la eficacia de la seguridad

¿Cómo se puede reducir y administrar el riesgo en un mundo de aplicaciones por todas partes y usuarios en cualquier lugar? Incrementando su "Eficacia de la seguridad".

Incrementar la eficacia de la seguridad significa fortalecer sus capacidades para...

## **Defenderse** contra tantos ataques como sea posible, entre otros:

- Ataques a aplicaciones web
- Malware
- Fugas de datos
- Ataques DoS y DDoS
- Ransomware

## **Identificar** los ataques que penetran las defensas lo más rápido posible, utilizando:

- Información de seguridad enriquecida y en tiempo real de una amplia gama de dispositivos de seguridad y de red
- Datos contextuales acerca del usuario, la red y comportamiento del sistema
- Aprendizaje automático
- Análisis avanzado de amenazas

## **Responder** eficazmente, mediante:

- Identificación y resolución de las vulnerabilidades y las anomalías de seguridad
- Parcheo automatizado
- Actualización dinámica de políticas

En las próximas secciones de este libro electrónico consideramos cómo mejor puede Defender, Identificar y Responder.

# Defenderse contra ataques a aplicaciones web

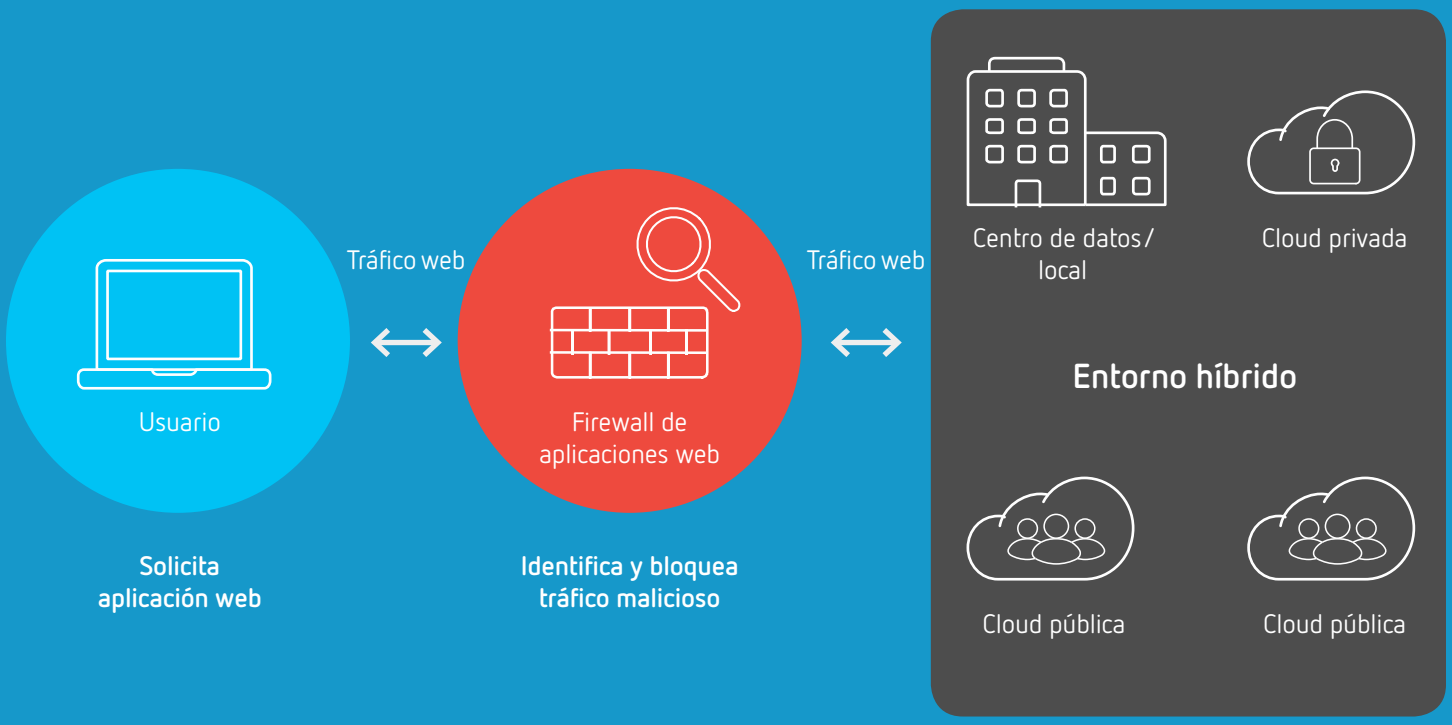
Un informe reciente de Verizon reveló que los ataques a las aplicaciones web representaron más del 40% de los incidentes resultantes de una violación de datos, y causaron la pérdida de más datos que cualquier otro tipo de ciberataque.*

Muchos ataques a aplicaciones web emplean técnicas bien conocidas, tales como la inyección de SQL y cross-site scripting. Otros explotan los servidores deficientemente configurados y el software mal diseñado de autentificación y gestión de sesiones. Por último, otros lanzan ataques de día cero contra vulnerabilidades recién descubiertas en populares paquetes de software web.

La clave de la defensa contra ataques a aplicaciones web es el firewall de aplicaciones web (WAF).
Un WAF proporciona seguridad centralizada a la capa de aplicaciones para aplicaciones y servicios web. Se encuentra entre los clientes web y servidores, y analiza el tráfico de aplicaciones, usando firmas y patrones para detectar infracciones de las políticas de seguridad y una amplia gama de ataques a aplicaciones web. Esto incluye el reconocimiento y bloqueo de la mayoría de los riesgos de seguridad para aplicaciones web más importantes de la lista "OWASP Top 10", creada por el Open Web Application Security Project.

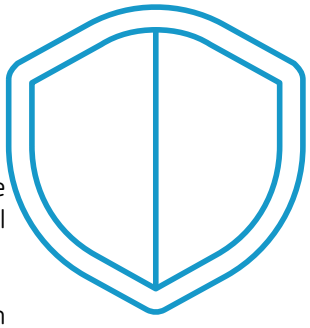
Un firewall de aplicaciones web también pueden proteger contra anomalías de las aplicaciones y ataques de día cero mediante la creación dinámica de perfiles de comportamiento de las aplicaciones web y a advertencia de actividades inusuales.

Además, un WAF puede ayudar a los administradores de red y seguridad a segmentar redes, de modo que solo los usuarios autorizados puedan tener acceso a aplicaciones clave. La segmentación de red mejorada ayuda a las empresas a cumplir con regulaciones tales como PCI DSS, HIPAA, y el GDPR de la UE.




*2016 Data Breach Investigation Report, de Verizon

# Defenderse contra los ataques DDoS



Los ataques distribuidos de denegación de servicio (DDoS) pueden bloquear sitios web e interrumpir los procesos del negocio. Se están volviendo más frecuentes cada año. Un estudio encontró que casi la mitad de las organizaciones empresariales, gubernamentales y educativas experimentan más de 10 ataques de DDoS al mes.*

Afortunadamente, los firewalls de aplicaciones web ofrecen una amplia variedad de funciones de protección DDoS tales como:

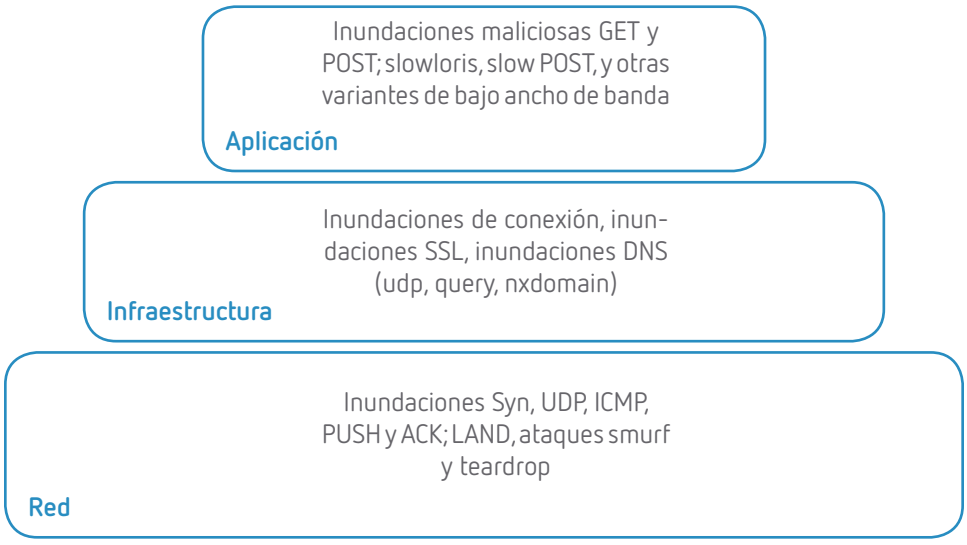
- Validación del protocolo
- Limitación de la velocidad
- Balanceo de carga

Estas y otras capacidades ayudan a los WAF a detectar y mitigar los ataques DDoS al nivel de red y de infraestructuras, que inundan los servidores web con paquetes de red inútiles. Algunas también pueden atenuar los sofisticados "bajos y lentos" ataques DDoS de nivel de aplicación, que se aprovechan de las debilidades de las aplicaciones web para saturar los servidores web y de base de datos.

La protección DNS puede atenuar los ataques que intentan inundar los servidores DNS y evitar que los usuarios accedan a sitios web externos.

Un servicio de reputación IP de amenazas es otra potente herramienta contra los ataques DDoS. Este servicio recoge y comparte información de una gran comunidad de empresas sobre sitios web y botnets que son controlados por los hackers y ciberdelincuentes. Armado con esta información, un WAF puede terminar todas las sesiones de estas direcciones IP maliciosas antes de que interfieran con las operaciones de la empresa.

## Tipos de ataques DDoS




*12th Annual Worldwide Infrastructure Security Report, Arbor Networks

# Defenderse contra el malware y el tráfico web malicioso

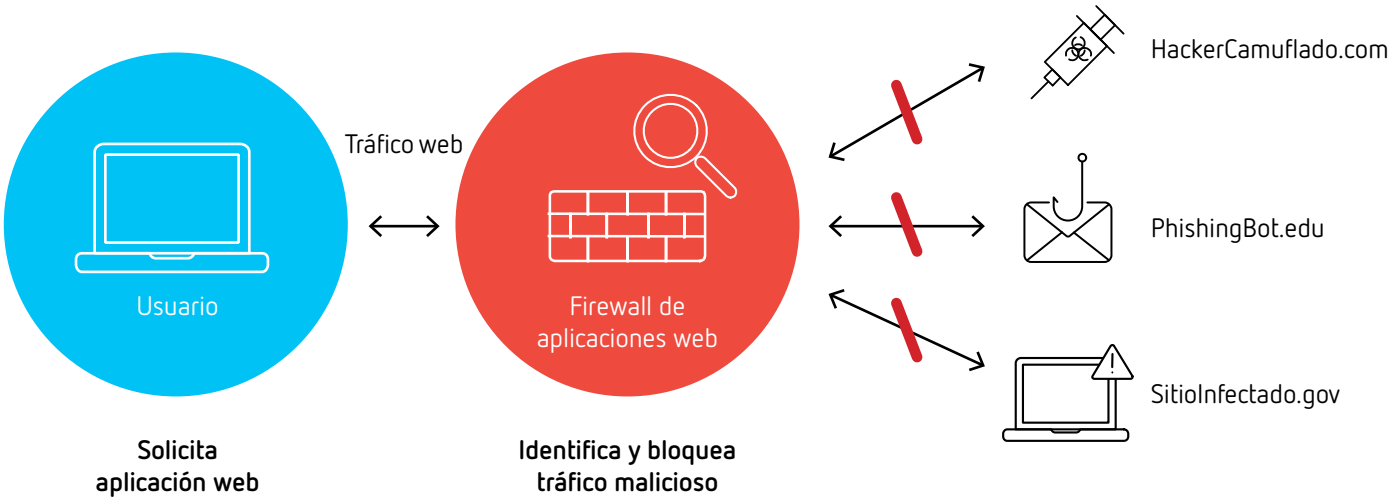
Muchos de los ataques dañinos más avanzados comienzan con un malware que llega a los dispositivos de los usuarios, ya sea como archivos adjuntos a mensajes de correo electrónico, o como descarga desde un sitio web bajo el control del atacante.

**Secure Web Gateway (SWG)** puede ayudarle a protegerse contra muchos de estos ataques web.

**El filtrado de URL** impide que los usuarios puedan navegar en sitios web que se sabe que están bajo el control de hackers y ciberdelincuentes y contaminarse inadvertidamente con malware. También previene que los empleados sean atraídos por correos electrónicos de phishing a sitios web en peligro donde revelan las credenciales de inicio de sesión e información personal.

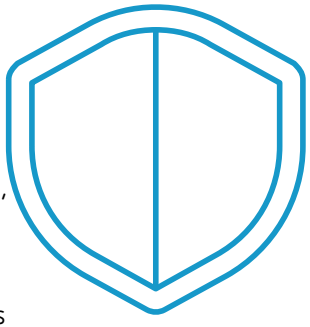
El filtrado de URL también ayuda a las organizaciones a cumplir con los requisitos de CIPA (Ley de Protección de la infancia en Internet) y regulaciones similares. CIPA requiere que las escuelas, bibliotecas y otros organismos eviten que los menores accedan a sitios web con materiales que son inapropiados para su edad.

**El descifrado de alta velocidad del tráfico SSL** permite a las organizaciones gestionar de forma segura grandes volúmenes de tráfico web cifrado. Esto es fundamental, ya que más de la mitad del tráfico web actual está cifrado.* Una Secure Web Gateway puede descifrar el tráfico SSL y escanearlo en busca de malware y firmas de ataque. También puede proteger los datos para garantizar que el tráfico saliente está cifrado, incluso si el cifrado SSL no se hubiera integrado en las aplicaciones originales.




*Google Transparency Report (actualizado online)

# Defenderse contra el acceso no autorizado



Los hackers y los ciberdelincuentes han encontrado que la manera más fácil de entrar en una red normalmente es capturar las credenciales de inicio de sesión y suplantar a los usuarios legítimos. De hecho, Verizon informa de que el 81% de las infracciones relacionadas con el hacking aprovecharon contraseñas robadas o débiles.*

Para gestionar el riesgo sin interrumpir los procesos empresariales, los departamentos de TI y los responsables de seguridad deben garantizar que:

- A las aplicaciones *solo* pueden acceder los usuarios autorizados
- Los usuarios autorizados pueden *acceder* siempre a las aplicaciones que necesiten, sin importar dónde estén y qué dispositivo estén utilizando

El éxito en este equilibrio requiere una inversión considerable en tecnologías de administración de identidad y acceso (IAM).

Por ejemplo, los gateways web pueden:

- Ofrecer **autentificación multifactor** y **registro único (SSO)** para usuarios en todos sus dispositivos, y todas sus aplicaciones, en cualquier lugar del mundo en el que puedan estar trabajando.
- Emplear **el control de acceso centralizado** y **la segmentación de la red** para proteger las aplicaciones y los datos críticos del acceso no autorizado.
- Proporcionar servicios de **auditoría** y **análisis de seguridad** por medio de la captura y el análisis de información detallada sobre el tráfico de las aplicaciones y sobre eventos tales como peticiones de acceso incorrectas.


*2017 Data Breach Investigation Report, Verizon

# Identificar los ataques que se cuelan lo más rápido posible

TI y los responsables de la seguridad ya no esperan poder bloquear todos los ataques que llegan a su red. A fin de aumentar la eficacia de la seguridad, necesitan poder identificar aquellos ataques que se cuelan reconociendo rápidamente los indicadores de peligro y los comportamientos anómalos.

Las herramientas de análisis de seguridad puede ayudar a las organizaciones a:

- Identificar y vigilar a los usuarios y las aplicaciones más atacadas.
- Identificar indicadores de peligro y pruebas de actividad maliciosa, como el tráfico de la red a los sitios web y los botnets controlados por hackers, solicitudes de acceso denegadas e intentos de ataques a aplicaciones web.
- Señalar comportamientos de riesgo y anómalos de los empleados, contratistas y otras personas con acceso a información privilegiada (y de los atacantes que utilicen sus credenciales), tales como la navegación inapropiada por la web, el exceso de acceso a los archivos confidenciales y los intentos de transferir datos a dispositivos de almacenamiento no seguros.
- Reconocer el tráfico de red anómalo, como los volúmenes inusuales de datos cargados y descargados, y picos de tráfico que indican ataques DDoS incipientes.

Las soluciones de análisis de seguridad avanzadas van mucho más allá de simplemente generar alertas: Ellos:

- Recopilan y correlacionan datos procedentes de una amplia gama de fuentes, como aplicaciones de escritorio y dispositivos móviles, aplicaciones web y microservicios, y dispositivos de seguridad y middleware
- Permiten a los analistas entender rápidamente las pautas y las tendencias de los usuarios, aplicaciones, dispositivos y redes con la ayuda de paneles y herramientas de visualización
- Emplean aprendizaje automático e inteligencia artificial para identificar sutiles comportamientos anómalos y encontrar patrones sospechosos en indicadores de compromiso aparentemente no relacionados.

Estas capacidades ayudan a los analistas de seguridad y red a eliminar puntos débiles y detectar antes los ataques en curso, antes de que puedan poner en peligro los datos y los procesos empresariales.


Clientes con la mayoría de las infracciones de seguridad

Aplicaciones bajo ataque

Principales ubicaciones de ataque

Tendencias de ataque

# Responder con eficacia a las amenazas

La identificación de ataques no es suficiente. Las organizaciones deben ser capaces de detener los ataques en curso y, luego, corregir las vulnerabilidades de modo que los ataques no vuelvan a repetirse en el futuro.

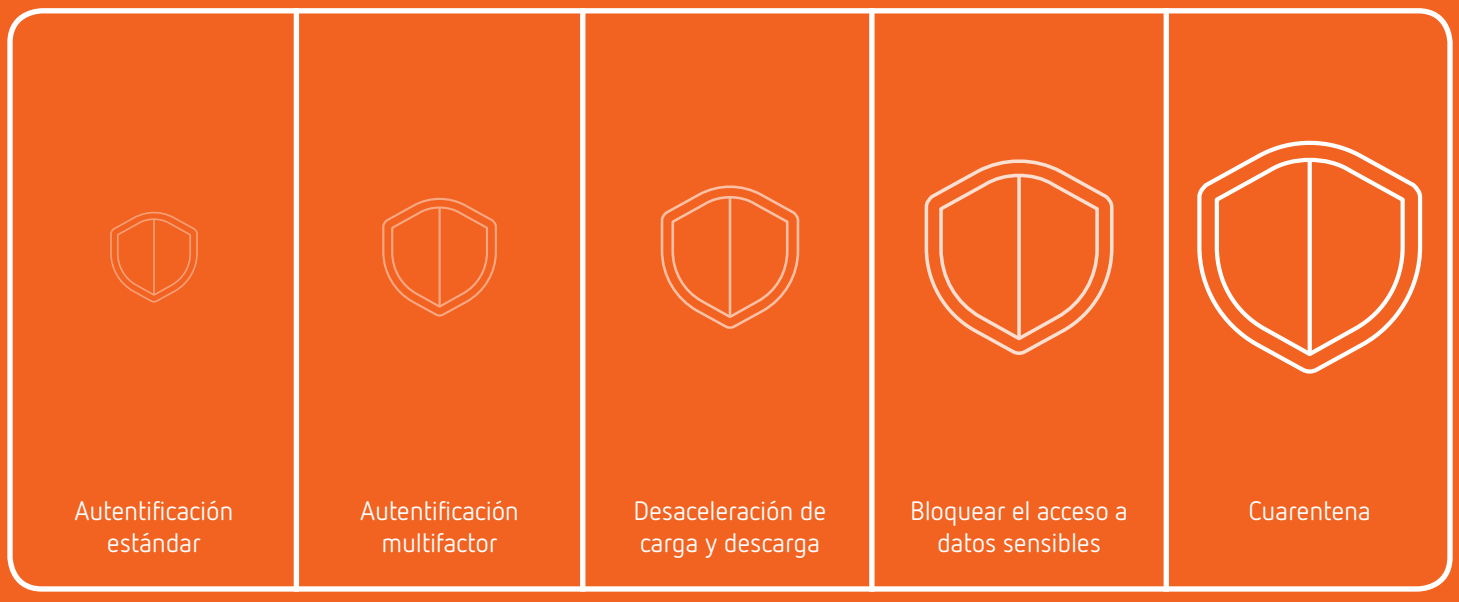
Después de reconocer ataques, algunas herramientas de análisis de seguridad avanzada pueden cerrar el bucle tomando pasos automáticos para aumentar progresivamente las defensas. Por ejemplo, cuando es evidente que una cuenta de usuario puede estar en peligro, una herramienta podría:

- En primer lugar, requerir la autentificación multifactor para el acceso a las aplicaciones
- Luego reducir el volumen de datos que el usuario pueda descargar y cargar
- Después bloquear el acceso del usuario a las aplicaciones que contienen datos confidenciales
- Y finalmente, poner en cuarentena al usuario, impidiendo que se acceda o se envíe cualquier dato fuera de la red.

Este control granular sobre las políticas de seguridad evita la fuga de datos, minimizando la posibilidad de que los usuarios no puedan hacer un trabajo legítimo.

Además, una herramienta de corrección de vulnerabilidades de aplicaciones web puede permitir a las organizaciones responder rápidamente a vulnerabilidades recientes. Distribuyendo rápida y fiablemente actualizaciones de políticas y parches a sistemas vulnerables, puede impedirse que los ataques de día cero se afiancen en la red.

## Análisis que aumentan progresivamente las defensas



# Requisitos generales: Visibilidad y protección integral

Para protegerse a sí mismos en una era cada vez más compleja de infraestructuras informáticas, las organizaciones necesitan soluciones que les permitan gestionar más tecnologías de seguridad, a través de una amplia gama de instalaciones y plataformas cloud, con menos administradores y personal de soporte técnico.

Hoy en día, la eficacia de la seguridad exige:

**Visibilidad y control desde el centro de datos a la nube,** de manera que las organizaciones puedan proteger entornos híbridos que se expandan por centros de datos locales y nubes públicas y privadas.

**Soluciones de seguridad integradas** de modo que las organizaciones puedan defenderse contra una amplia gama de amenazas sin tener que crear y mantener interfaces personalizadas y conectores.

**Administración centralizada,** así un mínimo personal puede implementar y mantener un conjunto coherente de políticas de seguridad a través de varias tecnologías de seguridad y entornos informáticos, y regiones globales.

**Análisis completo de seguridad,** de modo que las organizaciones puedan detectar amenazas a la seguridad avanzadas, sutiles y multivector.

Esta combinación no solo simplifica la gestión y reduce los costes, sino que también aumenta considerablemente la capacidad de una organización para implementar y modificar con confianza las aplicaciones.




# Cómo incrementa la eficacia de su seguridad Citrix® NetScaler® Security Portfolio

Las soluciones de seguridad de Citrix NetScaler Security Portfolio le permiten reducir y gestionar el riesgo de su negocio. Puede aumentar la eficacia de su seguridad rápidamente sin ampliar su personal.

## Defenderse contra ataques a aplicaciones web

**NetScaler AppFirewall™** y **NetScaler Web App Security Services®** utilizan firmas y diseños para **defenderse contra los ataques conocidos de aplicaciones web**. También emplean perfiles dinámicos de comportamiento de aplicación web para reconocer y **protegerse contra anomalías de las aplicaciones y ataques de día cero**.

**NetScaler AppFirewall** también proporciona **funciones de segmentación de red** que mantienen alejados a los intrusos de las aplicaciones clave. Esto refuerza el **cumplimiento de normativas**, así como la seguridad.

## Defenderse contra ataques de red

**NetScaler ADC** incluye la protección **DDoS y DNS** incorporada que **lo defiende de ataques de red**. Las técnicas como la limitación de la velocidad, el balanceo de carga y el análisis del tráfico de las aplicaciones web pueden mitigar los ataques DDoS en todos los niveles – aplicación, infraestructura y red – y mantener el funcionamiento de los servicios DNS. Otra característica incorporada, el **servicio de reputación IP de NetScaler**, cierra las conexiones desde direcciones IP con mala reputación.

## Defenderse contra el malware y el tráfico web malicioso

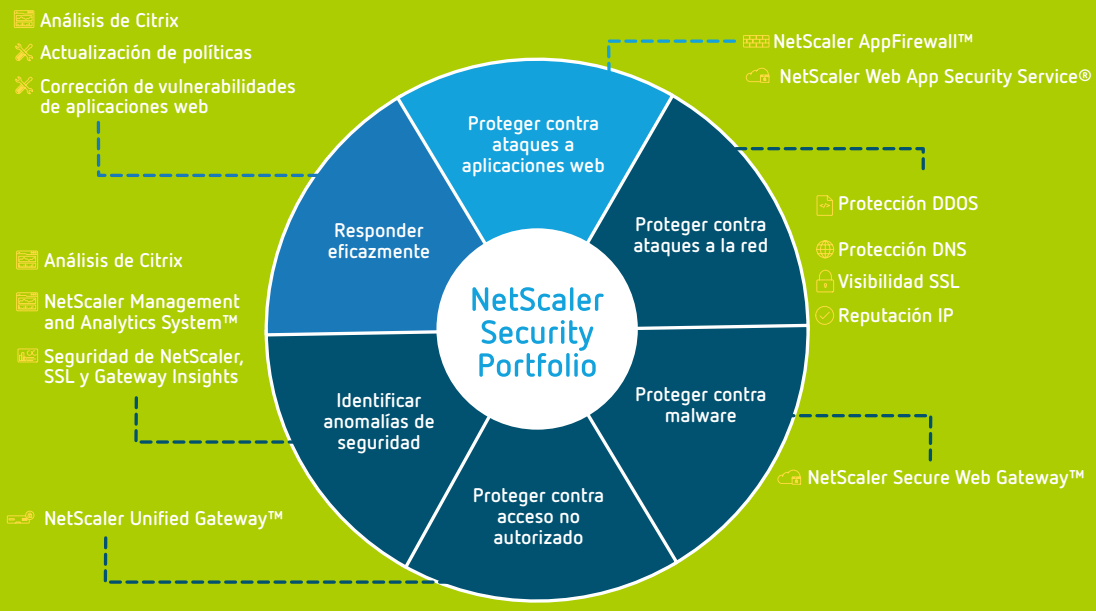
**NetScaler Secure Web Gateway™** le ayuda a **defenderse contra el malware y el tráfico web malicioso**. **NetScaler URL Threat Intelligence** bloquea el acceso a sitios web utilizados para ataques de phishing y descargas drive-by o malware. **El descifrado a alta velocidad del tráfico SSL** hace que sea posible detectar malware y tráfico malicioso ocultos por el cifrado SSL.

## Defenderse contra el acceso no autorizado

**NetScaler Unified Gateway™** ayuda a las organizaciones **a defenderse del acceso no autorizado** a aplicaciones y datos clave. Proporcionar tecnologías clave de identidad y de administración de acceso tales como **autentificación de múltiples factores** y **registro único**. También ofrece **control de acceso centralizado**, **segmentación de red** y **auditoria**.

## Identificar ataques tan pronto como sea posible

Citrix Analytics, junto con NetScaler Management y Analytics System (MAS), y NetScaler Security, SSL y Gateway Insights permiten a los analistas de seguridad y red identificar los ataques en curso. Capturan datos de una amplia gama de dispositivos y redes, proporcionan paneles y herramientas de visualización de datos, y utilizan aprendizaje automático e inteligencia artificial para encontrar patrones y resaltar las desviaciones de esos patrones. Mediante la identificación de indicadores de riesgo y la indicación de comportamientos anómalos y peligrosos, estas herramientas analíticas de seguridad avanzadas permiten determinar con mayor rapidez y confianza si un ataque real está teniendo lugar.




## Responder con eficacia a las amenazas

Citrix Analytics no solo ayuda a identificar y analizar las amenazas, sino que también le proporciona una herramienta para cerrar el bucle aumentando progresivamente las defensas en niveles acordes con el riesgo. Por ejemplo, a medida que se descubren otros indicadores de riesgo y se asocian con un usuario, usted puede aplicar automáticamente métodos de autentificación más rigurosos, reducir el acceso del usuario a la información o incluso poner en cuarentena al usuario.

El porfolio de Citrix NetScaler o las soluciones de seguridad también incluyen herramientas de corrección de vulnerabilidades de aplicaciones web que le permiten responder a vulnerabilidades recién descubiertas mediante la rápida distribución y aplicación de actualizaciones de políticas y parches.

## Disfrutar de visibilidad y protección integral

Por último, Citrix le ayuda a aumentar la eficacia de la seguridad frente a la ampliación de las áreas de ataque, una mayor complejidad y presupuestos ajustados. El porfolio de seguridad de NetScaler le ofrece:

- Visibilidad y control desde el centro de datos a la nube
- Un porfolio de soluciones de seguridad integradas
- Administración centralizada y, por último,
- Análisis total de la seguridad

**Descubra más sobre la eficacia de la seguridad**
http://now.citrix.com/security-efficacy